Some Approaches to for Testing Irreducibility in $\mathbb{Q}[x]$

On a couple of qualifying exams, you were asked to show that $f(x) = x^5 - 9x + 2$ is irreducible over $\mathbb{Q}$. This polynomial isn't immediately p-Eisenstein for any selection of p. One variation to this approach that you've surely encountered is applying the Eisenstein criterion to a shifted version of the polynomial, (e.g. apply the Eisenstein criterion to $f(x + a)$ where a is some integer). As it turns out, this doesn't help in this case (no integer shift $-1000 \leq a \leq 1000$ helps). What follows is a fairly general approach (along with a particular trick relevant to this problem). For this write up, we'll denote the ring $\mathbb{Z}/p\mathbb{Z}$ as $\mathbb{Z}_p$.

We first note that ±1 and ±2 aren't roots of $f(x)$, so by the rational roots theorem $f(x)$ has no rational roots, and thus $f(x)$ has no linear factors over $\mathbb{Q}$.

We can gain insight into $f(x)$ by mapping $f(x) \in \mathbb{Z}[x]$ to a corresponding polynomial $\tilde{f}(x) \in \mathbb{Z}_p[x]$ (for some fixed prime p) by sending each coefficient of $f(x)$ to its reduction mod p. More formally we use the map $\Phi_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$, the ring homomorphism induced by the reduction ring homomorphism $\phi_p : \mathbb{Z} \to \mathbb{Z}_p$, defined so that the monomial $\Phi_p(a_j x^j) = \phi_p(a_j)x^j$ (and then extending linearly). If the polynomial $\tilde{f}(x) = \Phi_p(f(x))$ is of the same degree as $f(x)$ and is irreducible in $\mathbb{Z}_p[x]$, then $f(x)$ is irreducible in $\mathbb{Z}[x]$.[1] This can be used directly if we consider the reduction mod 7, but this approach resolves in an unfortunate argument involving an obnoxious number of cases. Another approach is to note that by the contrapositive of the above statement, you have that if $f(x)$ is reducible, then $\Phi_p(f(x))$ is reducible; indeed if $f(x) = h(x)g(x)$ then $\Phi_p(f(x)) = \Phi_p(h(x))\Phi_p(g(x)) = \tilde{h}(x)\tilde{g}(x)$.

We proceed by applying $\Phi_3(f(x)) = x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$. Letting $a(x) = x^4 + x^3 + x^2 + x + 1$, we see that $a(x)$ has no linear factors in $\mathbb{Z}_3[x]$ (just plug in all values from $\mathbb{Z}_3$), so if it is reducible, it must factor into a product of irreducible quadratic polynomials. Again, we could go through the tiresome process of ruling out this possibility, but there is a better way.

Recall that when k is a field and $P(x)$ is a polynomial in $k[x]$, we know that $P(x)$ has a root $\alpha \in \overline{k}$ (some fixed algebraic closure of k) such that $k[\alpha]/k$ is a degree d extension if and only if $P(X)$ has a degree d polynomial factor which is irreducible over k.

Working towards a contradiction, we'll assume that $a(x)$ is reducible, and thus (by the above) factors into a product of two irreducible quadratic polynomials. We then take $\alpha \in \overline{\mathbb{Z}_p}$, such that α is a root of $a(x)$. This α would then induce a quadratic field extension $K = \mathbb{Z}_3[\alpha]$; this K would then have 9 elements, one of which is α. This $\alpha \in K$ is a root of $a(x)$, so it is also a root of $\tilde{f}(x)$, and thus $\alpha^5 = 1$. This tells us that α has group order 1 or 5 in $K^\times$. Clearly, $\alpha \neq 1$, so α must have group order 5 in $K^\times$. This is a contradiction, as the group $K^\times$ has 8 elements, so by Lagrange's theorem cannot have any elements of order 5. We thus see that $a(x)$ is irreducible.

Now working towards another contradiction, we assume that $f(x)$ is reducible. We then know that there exist monic non-constant polynomials $g(x)$ and $h(x)$ so that $f(x) = g(x)h(x)$ and thus $\phi_p(f(x)) = \phi_p(g(x))\phi_p(h(x)) = \tilde{g}(x)\tilde{h}(x)$. Clearly $\tilde{g}(x)$ and $\tilde{h}(x)$ are non-constant monic polynomials whose degrees sum to 5. As $\mathbb{Z}_p[x]$ is a unique factorization domain, we then have $a(x)$ divides $\tilde{g}(x)$ or $\tilde{h}(x)$; WLOG, say it divides $\tilde{h}(x)$. We then find that $\tilde{g}(x)$ is linear, and so $g(x)$ is linear. This is a contradiction, as we had already found that $f(x)$ has no linear factors. We thus conclude that $f(x)$ is irreducible.

[1] Please note, the converse is not true! For example, the polynomial $x^4 + 1$ is reducible mod every prime, but is (fairly clearly) irreducible over $\mathbb{Q}$.